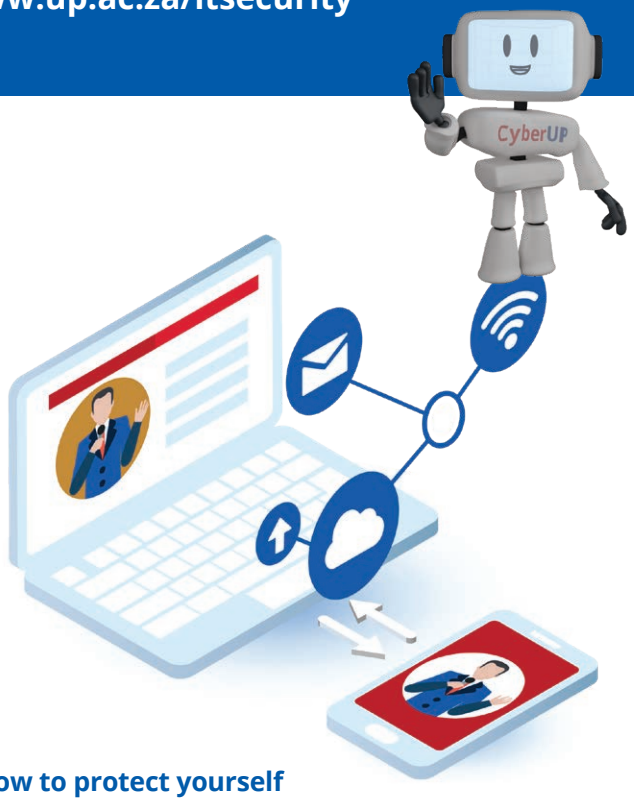
UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Information Technology Services

Information and Cybersecurity Awareness

Email ithelp@up.ac.za | **www.up.ac.za/itsecurity**



Wi-Fi security

'Make your home a haven for online security'

Security for most residential estates starts at the gate providing access to the estate. The entrance is the first line of defence against visitors with dubious intent seeking access to the homes, vehicles and valuable assets inside the perimeter. Each home inside may have its own additional security measures, but everyone will be safer if there is some form of central control over who enters the premises.

Introduction

Your Internet router is the gateway for all traffic between your home network and the Internet. It is the first line of defence for guarding against attacks on your home devices connected to the Internet, which may include computers, phones, smart TVs, security cameras and appliances. The router is prone to attacks by cybercriminals. Should their exploits succeed, they could retrieve sensitive information from your devices, redirect your traffic to fraudulent websites, or intercept communication between two parties and alter its content by injecting malicious code or replacing information like bank details. A lack of security could also enable strangers to use your router and data to access the Internet, sometimes for dubious purposes like sending spam or committing crime.

SEE MORE

5 easy ways to secure your home Wi-Fi network

READ MORE

Securing your wireless network
How to secure your personal Wi-Fi router

DO MORE

Take responsibility for your home network

How to protect yourself

1. Secure access to the router settings
Change the default administrator password on the router to a strong, unique password.

2. Review the router settings
The manufacturer of your router may have already set up default, basic security requirements on your router. However, you should review the settings to ensure that they meet your own requirements.

- Ensure that the Wi-Fi name (SSID) is something unique that preferably does not identify you as the owner.
- Consider not broadcasting the SSID. This would require you to provide the SSID to anyone wishing to use your Wi-Fi network.
- Ensure that traffic between the router and your devices is encrypted using the strongest possible encryption level (currently WPA2-PSK).
- Select a strong, unique password to allow access to the Wi-Fi network.
- Enable automated updates for your router's firmware (operating system).

Instructions on how to do the above should be available on the manufacturer's website. The resources listed under 'SEE MORE' and 'READ MORE' also contain general advice in this respect.